

No. 793719

RECEIVED  
SUPREME COURT  
STATE OF WASHINGTON  
2007 MAR -5 P 1:45

IN THE SUPREME COURT  
OF THE STATE OF WASHINGTON

*h/h*  
CLERK

---

STATE OF WASHINGTON,

Petitioner/Respondent,

v.

MICHAEL ALLAN BOYD, Petitioner,

LEE GILES, Respondent,

MAUREEN ELIZABETH WEAR, Respondent

---

ANSWER TO STATE'S MOTION TO STRIKE

---

Sheryl Gordon McCloud  
WSBA No. 16709  
Law Offices of Sheryl Gordon  
McCloud  
710 Cherry Street  
Seattle, WA 98104-1925  
(206) 224-8777  
Attorney for Amicus NACDL

Colin Fieman  
Georgia Bar No. 259690  
1331 Broadway, Suite 400  
Tacoma, Washington 98402  
(253) 593-6710  
Attorney for Amicus WACDL

Laura E. Mate  
WSBA No. 28637  
1601 Fifth Ave., Suite 700  
Seattle, WA 98101  
(206) 553-1100  
Attorney for Amicus WACDL

## **I. INTRODUCTION**

Amici, Washington Association of Criminal Defense Lawyers (WACDL) and National Association of Criminal Defense Lawyers (NACDL) oppose the State's motion to strike portions of its brief and all of its appendices.

## **II. ARGUMENT**

The State relies on RAP 10.3(a) to argue the appendices and references thereto should be stricken. This rule, however, gives this Court the discretion to allow an appendix to include materials not in the record. RAP 10.3(a)(8) ("An appendix may not include materials not contained in the record on review *without permission from the appellate court*") (emphasis added). Given the nature of amici's brief and appendices, the Court should exercise its discretion to allow the appendices.

The appendices are not offered as specific facts of this case, but instead as illustrative examples to amici's discussion of the practice in state and federal courts, as well as the rationale for that practice. *See State ex rel T.B. v. CPC Fairfax Hosp.*, 129 Wn.2d 439, 918 P.2d 497 (1996) (denying motion to strike appendices containing scholarly articles where authorities understood not as "establish[ing] the specific facts of this case

but rather [as] ‘legislative facts’ which the court may consider when determining the constitutionality or interpretation of a statute”). This information is offered to provide the Court context and an understanding of the potential impact of the different rulings it could make in these consolidated cases.

In addition, Appendices B-F all are signed and filed orders in federal and state courts. While RAP 10.4(h) prohibits citing as authority unpublished opinions of the Court of Appeals, there is no rule prohibiting citation to unpublished decisions of state and federal trial courts. *See, e.g., Anderson v. King Cy.*, 158 Wn.2d 1, 154, 138 P.3d 963, 213 n. 29 (2006) (Fairhurst, J. dissenting) (citing unpublished trial court decision from Alaska); *Dwyer v. J.I. Kislak Mortgage Co.*, 103 Wn. App. 542, 548-49 (imposing sanctions for citation of unpublished decision of Washington Court of Appeals, but not for extensive citation of unpublished trial court decisions). Similarly, RAP 10.4(h) does not bar citation to unpublished decisions for some reason other than legal authority. Here the appended decisions are offered not as legal authority nor as specific facts to this case, but to explicate and illustrate alternative procedures that trial courts may use to avoid the objections raised by the State.

In response to the State's concern with Appendix A, we are attaching to this Answer an affidavit of Marcus Lawson that is almost identical to that filed in App. A. This affidavit is signed by Mr. Lawson and was filed in King Co. Superior Court No. 06-1-06626-6 SEA on January 10, 2007.

Should this Court decline to exercise its discretion and allow the appendices, amici requests this Court continue argument on this case and remand to allow the parties to further develop the record pursuant to RAP 9.11.

### **III. CONCLUSION**

To properly determine the scope of a ruling in these consolidated cases, the information about the practice in state and federal courts, as well as the rationale for that practice is critically important. The Court has discretion to consider this material under the circumstances it is presented, and amici urges it to do so. In the alternative, amici requests this Court continue argument to allow further development of the record pursuant to RAP 9.11.

//

//

DATED this 5<sup>th</sup> day of March, 2007.

Respectfully submitted,

/s/  
Sheryl Gordon McCloud  
WSBA No. 16709  
Attorney for Amicus NACDL

/s/  
Colin Fieman  
Georgia Bar No. 259690  
Attorney for Amicus WACDL

/s/  
Laura E. Mate  
WSBA No. 28637  
Attorney for Amicus WACDL

## CERTIFICATE OF SERVICE

I certify that on the 5th day of March, 2007, a true and correct copy of the foregoing ANSWER TO STATE'S MOTION TO STRIKE, was served upon the following individuals by depositing same in the United States Mail, first class, postage prepaid:

Barbara L. Corey  
Attorney for Petitioner Michael Allan Boyd  
901 S. I St., Suite 201  
Tacoma, WA 98405

Michael Schwartz  
Attorney for Respondent Lee Giles  
524 Tacoma Ave. S.  
Tacoma, WA 98402

Mary K. High  
Attorney for Respondent Maureen Elizabeth Wear  
949 Market St., Suite 334  
Tacoma, WA 98402

Gerald R. Horne  
Pierce County Prosecuting Attorney  
Kathleen Proctor  
Pierce County Prosecutor's Office  
Hugh Birgenheier  
Pierce County Prosecutor's Office  
930 Tacoma Ave. S., Rm. 946  
Tacoma, WA 98402  
Counsel of Record for the State

CLERK

RECEIVED  
SUPREME COURT  
STATE OF WASHINGTON  
2007 MAR -5 P 1:45

/s/

Sheryl Gordon McCloud

1 RECEIVED THE HONORABLE CATHERINE SHAFFER  
2 07 JAN 10 PM 3:53  
3 KING COUNTY  
4 SUPERIOR COURT CLERK  
5 SEATTLE, WA

6 IN THE SUPERIOR COURT OF THE STATE OF WASHINGTON  
7 IN AND FOR THE COUNTY OF KING

8 STATE OF WASHINGTON,

9 Petitioner,

10 v.

11 Respondent.

No. 06-1-06626-6 SEA

MOTION TO RELEASE EVIDENCE  
FOR COMPREHENSIVE  
EXAMINATION BY DEFENSE  
EXPERT

12 COMES NOW the defendant, [REDACTED] by and through his attorneys, John  
13 Henry Browne and Jessica Riley, and moves this Court pursuant to CrR 4.7 for an order  
14 releasing the State's evidence into the custody of the defendant's expert for the purpose  
15 of conducting an independent comprehensive examination. This motion is based on the  
16 following facts and circumstances, the attached sworn declaration, and the records and  
17 files herein.

18 Attached hereto in support of this motion are the Curriculum Vitae of Marcus  
19 Lawson (Exhibit A), and the sworn declaration of Marcus Lawson President of Global  
20 CompuSearch, LLC (Exhibit B), which addresses the basis upon which this Motion is  
21 being made.

22 FACTS

23 The defendant, [REDACTED] is currently charged with Count I, Child Molestation  
24 in the First Degree – Domestic Violence; Count II, Rape of a Child in the Second Degree

MOTION FOR RELEASE OF EVIDENCE FOR  
COMPREHENSIVE EXAMINATION BY  
DEFENSE EXPERT 1

ORIGINAL

LAW OFFICES OF JOHN HENRY BROWNE, P.S.  
2100 EXCHANGE BUILDING  
821 SECOND AVENUE

# **Exhibit B**



## AFFIDAVIT OF MARCUS LAWSON

I, Marcus Lawson, President of Global CompuSearch LLC, do hereby depose and state:

### **Background**

1. I am the President of Global CompuSearch LLC, located in Spokane, Washington and have been so employed since July of 2000. Global CompuSearch LLC provides consulting, computer forensics and training services on legal issues related to computers and the Internet. The consulting work the company provides offers a special emphasis on sex crimes, child sexual abuse and child pornography issues involving the Internet.
2. Prior to my work at Global CompuSearch I was employed as a Special Agent with the United States Customs Service for twelve years. Previous to my employment with the Customs Service, I was employed as a Special Agent with both the Drug Enforcement Administration and U.S. Secret Service for five years. My education consists of a Bachelor of Science Degree in Administration of Justice from Portland State University and a Juris Doctor from Pepperdine University School of Law. During my employment with the United States Customs Service I investigated and worked as an undercover operative in cases of fraud, narcotics, weapons violations, terrorism and child pornography. For eleven of the twelve years I was a Special Agent with the Customs Service I specialized in the investigation of child pornography and child sexual abuse cases.
3. During my employment with the Customs Service I both received and provided extensive training in the areas of child pornography, the sexual abuse of children, and the behavior of pedophiles. I received training from the Customs Service, the United States Department of Justice, and other federal, state and local law enforcement agencies. I received instruction on investigations of child sexual exploitation from the Customs Service as well as training in the use of computers to obtain and distribute child pornography both from the Customs Service and SEARCH, The National Consortium for Justice Information and Statistics, Sacramento, California. I personally coordinated the Northwest Child Exploitation Conference on behalf of the Customs Service and served as an instructor in undercover techniques and case studies in the field of child exploitation and child pornography crimes. During my period of employment with United States Customs, I coordinated training seminars and trained at seminars coordinated by others, training federal, state and local law enforcement personnel in Oregon, Washington, Idaho, California, Utah, Montana, Alaska, Indiana and Michigan, the United States Attorneys Office, the Federal Public Defenders Office, the American Probation and Parole Officers Association, the Naval Investigative Service, the Federal Bureau of Investigation, the United States Postal Inspection Service, the United States Customs Service Cyber Smuggling Center and dozens of social service providers and community service groups.
4. In 1996 I created one of the first investigative manuals in use by law enforcement investigators and prosecutors outlining investigative techniques and strategies on the Internet. I assisted in the planning and creation of the U.S. Customs Cyber Smuggling Center in 1997.

I have also testified before the Oregon State Legislature on issues pertaining to the drafting of child pornography legislation. During my period of employment with the Customs Service I represented U.S. Customs child pornography investigative efforts in numerous print media and television interviews including NBC Nightly News, The Montel Williams Show and BBC Television.

5. During my employment with the United States Customs Service I personally coordinated four undercover child pornography sting operations and initiated child pornography and/or child exploitation investigations throughout the United States and the world. I coordinated these types of investigations with the Royal Canadian Mounted Police, Scotland Yard, the German Polizei, Naval Investigative Service, Army Criminal Intelligence Division, the Federal Bureau of Investigations and scores of state and local police agencies.
6. As President of Global CompuSearch, I continue to receive requests by both law enforcement and criminal defense entities for training on computer crime issues. As a result, since leaving the employ of the government, I have conducted training with sheriffs departments, police departments, state and federal parole officers associations, state and federal public defenders, state and federal public defenders investigators and private citizens groups.
7. As President of Global CompuSearch, I continue to investigate allegations of Internet crime. Since becoming a private consultant I have conducted examinations on well over two hundred computer hard drives and hundreds of other pieces of digital media, advising attorneys on findings and often comparing these findings with the reports of law enforcement forensics investigators.
8. I am also the head supervisor for Global CompuSearch and as such, review the findings and reports of all other forensics examiners employed by Global CompuSearch.
9. Global CompuSearch is an independent consulting firm and while the case load consists of many criminal defense issues, forensic examiners at Global CompuSearch do not act as defense advocates but rather act as factual advisors to the attorneys in these cases. Global CompuSearch forensic examiners report all findings to the attorneys regardless of whether those findings are inculpatory or exculpatory toward the attorney's client.
10. This firm's list of clients in these matters includes the United States Army, The United States Navy, The United States Air Force, The United States Marine Corps, Federal and State Public Defender Offices throughout the United States, private attorneys throughout the United States, Europe, and business entities throughout the United States and Europe. Global CompuSearch examiners have examined computer evidence in allegations of capital homicide, rape, child pornography, "traveling" for sex with minors, unauthorized access (hacking), arson, espionage and a host of other issues. Global CompuSearch forensics examiners regularly testify about their findings in courts throughout the United States and around the world.
11. The term "child pornography," as used in this declaration refers to visual depictions of minors engaged in sexually explicit conduct. The terms "minor," "sexually explicit conduct,"

"visual depiction," and "production," as used in this affidavit, are defined in Title 18, United States Code, Section 2256, et seq. The term "computer", as used herein, is defined in Title 18, United States Code, Section 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

### History

12. Global CompuSearch was requested by The Law Offices of John Henry Browne, P.S. to conduct a computer forensics analysis of computer hard drives and related media and to advise in the preparation of the defense in the case of the State of Washington v. Oleg Gouts. I have reviewed the report from Jan Fuller, Computer Forensic Investigator for Redmond Police Department, provided in discovery in this case.
13. John Henry Browne has informed me that the prosecution has indicated an intent to oppose the defendant's request for discovery and production of a mirrored hard drive and duplicated computer media because of the passage of H.R. 4472, the Adam Walsh Child Protection and Safety Act of 2006. Specifically, Sec. 504 of that act which proposes to prevent defense counsel from temporarily obtaining mirror copies of digital media in preparation for trial when it contains images alleged by the government to be child pornography provided the government provides "reasonable access" to the media at government proscribed facilities.
14. It is anticipated that I, or an investigator from my firm, would need to access the drive repeatedly to assist in the preparation of cross examination and/or possible testimony on his part as an expert witness for the defense.

### The Forensics Process

The examination and review of computer digital evidence is unlike any other type of evidence examination. It almost always involves the review of enormous amounts of data and often requires the use of multiple forensics tools to do so. This is true because of the following:

A. Volume of evidence: Computer storage devices ... can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence by storing it in random order with deceptive file names or deceptive file extensions. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks to months, depending on the volume of data stored. It would also be impractical to attempt this type of data search on site.

B. Technical requirements: Searching computer systems for criminal evidence is a highly technical process, requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, data search protocols are exacting

scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to inadvertent or intentional modification or destruction ... a controlled environment is essential to its complete and accurate analysis." (emphasis mine)

15. In a recent case handled by Global CompuSearch, the Texas Court of Appeals found reversible error when the State refused to provide a mirror copy of the defendant's hard drive for independent review, stating;

"In so holding, we disagree with the State's position that such a review must be conducted at a State-controlled facility. We would not require a chemist to take a "porta lab" with him or her into an evidence room to check alleged contraband drugs, and it is not appropriate to require a computer expert to carry his or her equipment into a State facility to review the documents." Taylor v. Texas (2002) WL 31318065.

16. Another recent child pornography case handled by this office was United States vs. Hill 322 F.Supp.2d 1081 (C.D.Cal. 06/17/2004). In a written opinion of Judge Alex Kozinski ruling in favor of a defense motion for discovery but discounting a defense contention that the law enforcement agents in that case should have done an "on-site" examination, he states;

"Even if the police were to bring with them a properly equipped computer, and someone competent to operate it, using it would pose two significant problems. ... Second, the process of searching the files at the scene can take a long time. To be certain that the medium in question does not contain any seizable material, the officers would have to examine every one of what may be thousands of files on a disk — a process that could take many hours and perhaps days. See pages 23-24 *infra*. Taking that much time to conduct the search would not only impose a significant and unjustified burden on police resources, it would also make the search more intrusive. ... "

17. Continuing in the opinion, Judge Kozinski went on to rule the defense, and specifically Global CompuSearch was entitled to mirror copies of the computer media containing contraband;

"Defendant wishes to obtain two "mirror image" copies of the computer media analyzed by the government's expert to allow his own expert to conduct a forensic analysis and his counsel to prepare his defense. The government opposes producing these items, offering instead to permit the defense to view the media in an FBI office and to conduct its analysis in the government's lab.

Federal Rule of Criminal Procedure 16(a)(1)(E) provides:

Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the

defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant.

Rule 16 clearly covers the items defendant has requested. They are "data, photographs, [and/or] tangible objects" within the government's possession. Moreover, they are material to the preparation of the defense, the government intends to use them in its case-in-chief and they were obtained from defendant. Rule 16(d)(1), however, allows the court to regulate discovery: "At any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief."

The government argues that since child pornography is contraband, defense counsel and his expert should be required to examine the images in the controlled environment of the government facility. The cases cited by the government, though, all involve appeals from district court decisions denying a defendant's motion to compel production. They do not hold that a district court would abuse its discretion if it were to order the government to produce copies of the materials.

The government analogizes the zip disks to narcotics, arguing that their inspection and analysis by defendant's expert should take place in the government's lab under government supervision. This analogy is inapt. Analysis of a narcotics sample is a fairly straightforward, one-time event, while a thorough examination of the thousands of images on the zip disks will take hours, even days, of careful inspection and will require the ability to refer back to the images as the need arises.

**The court concludes that defendant will be seriously prejudiced if his expert and counsel do not have copies of the materials.** Defense counsel has represented that he will have to conduct an in-depth analysis of the storage media in order to explore whether and when the various images were viewed, how and when the images were downloaded and other issues relevant to both guilt and sentencing. The court is persuaded that counsel cannot be expected to provide defendant with competent representation unless counsel and his expert have ready access to the materials that will be the heart of the government's case.

**The government's proposed alternative — permitting the defense expert to analyze the media in the government's lab at scheduled times, in the presence of a government agent — is inadequate.** The defense expert needs to use his own tools in his own lab. And, he cannot be expected to complete his entire forensic analysis in one visit to the FBI lab. It took defense counsel between two and three hours to quickly scroll through the 2,300 images in the Encase report, so it is likely to take the expert much longer than that to conduct a thorough analysis. **Defendant's expert is located in another state, and requiring him to travel repeatedly between his office and the government's lab — and obtain permission each time he does so — is unreasonably burdensome.** Moreover, not only does defendant's expert need to view the images, his lawyer also needs repeated access to the evidence in preparing for trial.

**There is no indication that defendant's counsel or expert cannot be trusted with the material.** The expert is a former government agent who has a safe in his office and

has undertaken to abide by any conditions the court places on his possession of the materials. He has experience in dealing with child pornography and takes precautions to ensure that contamination doesn't occur, including using the Encase software and fully "wiping" the forensic computers on which he examines the images. Defense counsel is a respected member of the bar of this court and that of the Ninth Circuit. The court has every confidence that he can be trusted with access to these materials." [Emphasis mine]

18. The resulting court order reproduced in the opinion states;

"2. The government shall provide defendant's expert, Marcus K. Lawson of Global CompuSearch, LLC, a copy of all of the Encase evidence files relating to this case, which includes evidence files for all media seized from [address deleted] on April 6, 2000, necessarily including any and all actual or alleged child pornography and/or contraband contained thereon. Mr. Lawson shall maintain and secure the Encase evidence files in the following manner:

a. Copies of the Encase evidence files shall be maintained by Mr. Lawson in accordance with this Order, and shall be used by Mr. Lawson solely and exclusively in connection with this case.

b. Copies of the Encase evidence files shall be maintained by Mr. Lawson in a locked safe in the offices of Global CompuSearch, LLC at all times, except while being actively utilized as provided for in this Order.

c. A copy of this Order shall be kept with the copies of the Encase evidence files at all times.

d. Copies of the Encase evidence files shall be accessed and viewed only by Mr. Lawson and staff employed by Global CompuSearch, LLC who Mr. Lawson has given this Order to and who agree to be bound by the requirements of this protective order.

e. Mr. Lawson shall maintain custody over the Encase evidence files and shall maintain a list of all Global CompuSearch, LLC employees granted access to the Encase evidence files.

f. Any computer into which copies of the Encase evidence files may be inserted for access and operation shall not be connected to a network while a copy of the Encase evidence files is inserted into any computer.

g. The computer into which copies of the Encase evidence files are inserted may be connected to a printer only under the following conditions: that any printer utilized is a local printer, that the printer may be connected only when and as necessary to print non-graphic image files, and that Marcus Lawson or staff employed by Global CompuSearch who are subject to this Order shall be personally present at all times a printer is connected.

h. In no event shall any graphic image containing actual or alleged child pornography be copied, duplicated, or replicated, in whole or in part, including duplication onto any external media.

3. Within 30 days of termination of this matter (including the termination of any appeal), defense counsel shall return (or cause the return of) copies of the retained computer evidence and the Encase evidence files to Special Agent Tim Alon or a representative of the Federal Bureau of Investigation. Upon the return of the copies of retained evidence and the Encase evidence files, defense counsel shall file a brief report to the Court specifying that the terms of this Order have been complied with and reporting the return of the copies of evidence.

IT IS SO ORDERED."

19. Just as discussed in the Hill opinion by Judge Kozinski, in order to assist John Henry Browne in his preparation of the defense of Mr. Gouts, it is likely to take me or an examiner from my office many hours to do even a preliminary analysis of the data found in the hard drive belonging to Mr. Gouts and will take him several more days of analysis to help prepare John Henry Browne for Mr. Gouts' trial. Without a repeated on-going, as needed access to Mr. Gouts' media, it simply is not possible for my firm to properly assist John Henry Browne in preparing for Mr. Gouts' trial.
20. In cases involving allegations of criminal misconduct, computer evidence is examined by law enforcement examiners, as was done here. It is the job of these police examiners to forensically examine the computer evidence given them looking for, and documenting, evidence of the criminal violation. Rarely (if ever) do police technicians examine this same evidence for exculpatory data that would assist the defense. Rather, if such evidence exists, it is deemed the responsibility of the defense team to find and document it. This is the investigative process of digital forensics.
21. Because computer evidence is by definition digital, and digital evidence is fragile, such evidence requires special forensics software tools for examination as well as the knowledge of how to use them correctly. Hence, computer evidence is virtually always examined in a controlled laboratory environment by trained personnel using specialized investigative software. Global CompuSearch has such a laboratory with a wide variety of forensic software available to its examiners, an up-to-date technical library, and different hard ware computer components for every operating system available as well as the combined technical knowledge of the four examiners employed here.
22. I can state from repeated experience that it is vitally important for the defense team to have the same access to the evidence in this case that the prosecution team has had and continues to have. As noted by Judge Kozinski, virtually every affidavit for search warrant filed by law enforcement officials seeking search warrants for computer related evidence, the computer forensics process takes considerable time and can not be done with any stated time

constraints as it is impossible to know beforehand the extent of the number and size of files available which may confirm or deny the allegations.

23. The standard of thoroughness in the examination process that Global CompuSearch examiners are required to maintain often requires the use of multiple forensics tools. These tools may be of a software or hardware nature. Some software is more useful for thoroughly examining specific areas of the computer than others. Sometimes a forensics program proves more appropriate for recovering text dialog than for recovering graphic images and another graphic-image program might recover specific files from specific locations in the computer better than another. In other words, the examination of computer data for evidentiary purposes is a dynamic process requiring multiple tools and substantial time and it is unreasonable to expect any competent computer examiner to bring his/her entire forensics laboratory including every software possibly needed and every computer hardware component possibly needed to a government proscribed location and then complete a detailed, thorough examination of the computer media under any kind of time constraint that would be financially and practically reasonable. In the course of the exam in this case it will likely be necessary to use multiple forensics software or other tools available in Global CompuSearch's laboratory which would be unavailable in a police controlled environment.
24. In the instant case, images have been alleged by the government to be visual depictions of minors in sexually explicit poses, in violation of federal law. Three issues that Global examiners take into consideration in all child pornography cases are:
  1. Whether the charged images do indeed meet the legal criteria for obscenity and/or child pornography.
  2. Whether their location within the computers hard drive tends to indicate a knowing possession by the defendant.
  3. The original source of the images and the context of their download.
27. Although not the only issues to be examined, these three issues in particular require personal observation of the drives themselves. Thus, independent examiners are required to examine not just the images themselves, but more importantly;
  - Their origination point from the Internet
  - Their path through the operating system to their present location
  - Their file date/time stamps which may or may not link specific computer use to the defendant or others.
28. Much of what passes as "computer forensics" in law enforcement entities devoted only to data recovery, is not investigative in nature at all. A field investigator sends these entities a seized computer. The technician at the facility makes a copy of the media and then extracts what the investigator asks them to extract. Little and often no investigative effort goes into the analysis of the seized drive.



29. Data recovery is the initial step in a computer investigation. The media needs to be copied correctly to ensure that a duplicate is created. Once that copy is created, it is up to the investigator to determine what evidence it contains. This is where the distinction begins. Many police computer forensics labs this firm has dealt with (and we have dealt with labs all over the country) will extract what the case agent or detective asks them to extract. In child pornography cases, this is usually limited to the suspect images and perhaps the Internet history files (which show world wide web browsing activity). This information is copied out and placed on CD Rom and given to the investigator.
30. In the experience of this firm, this approach usually leads to overlooked evidence, many times even overlooked evidence that would be extremely important to the prosecution of the case. While a layman might conclude that the technician extracting the data is performing "computer forensics", in actuality, all they have done is data recovery.
31. Computer forensics, at least as that term is applied in this office, is a great deal more than this. More accurately called computer investigations, when this firm receives a piece of media to examine, we examine all aspects of the information on it and are prepared to inform our clients of everything that is potentially relevant to their case. In other words, we investigate the media and determine what occurred, when it occurred, how it occurred and who was responsible for its occurrence. To answer these questions requires not just a working knowledge of data recovery, but a working knowledge of the Internet, it's applications, how offenses are committed with these applications, what types of behaviors are associated with which applications and a myriad of related issues.
32. But, in addition to that working knowledge, it also requires the ability of the examiner to be able to research new applications and programs on the fly as they are encountered during an examination. For example doing examinations in our own laboratory gives Global CompuSearch examiners live Internet access to research a new program or application. Similarly, doing exams in our laboratory gives these examiners access to our technical library as well as the expertise of other examiners to rely on to solve examination problems. The firm's laboratory also has test "mule" computers running various operating systems (Macintosh, Linux, and various versions of Windows) so that a new application or program can be run on the same operating system it was used on the defendant's machine to determine the nuances of how it works. It is simply a fact that various versions of various Internet applications and programs run differently, store data differently and react with the user differently depending not just on what operating system is used (Macintosh/Windows/Linux) but the different versions of those operating systems. None of these things are available in a government controlled facility nor would it be even remotely possible to bring these investigative tools to one.
33. For the government to assert that these types of resources can all be "loaded onto a laptop" and brought to a government office (as I was told recently by one federal agent) is either very naive or shows a lack of appreciation of what computer forensics actually entails. In reality what such an approach does is severely limit this firm's ability to know everything we need to know about a case, something the government is quick to exploit in the court room.

34. In the instant case, my firm's inability to have complete access to the media will prevent me or a forensic investigator from my firm from testifying as an expert should John Henry Browne wish him to do so simply because we will not have been able to prepare ourselves with the knowledge of the defendant's hard drive we would need to not just testify effectively for John Henry Browne but to withstand cross examination. Cross examination that will, no doubt, be assisted by Jan Fuller of the Redmond Police Department, who has had unlimited access to the hard drive in question, right up to the time of cross examination.
35. This type of thorough analysis is the same for every case this office handles. More than just our reputation, individuals liberties (and in some cases their lives) are at risk if we make mistakes or miss important evidence. The resources this firm has acquired, such as our test mule machines with various operating systems, have been acquired because they showed themselves repeatedly necessary for us to offer sound opinions to our clients. As a private firm, dependant on making a profit to survive, we have not acquired these expensive investigative tools lightly, rather, they are acquired because we need them to effectively perform our services. And, again, to believe that these types of assets can be "loaded onto a laptop" and carted around the country to various government facilities is simply not realistic.

#### **The Allegation of Child Pornography**

36. An important issue that should be noted is that it is merely the **allegation** that images are child pornography that triggers the act and its consequential restrictive access to discovery. In the six years that this firm has been in business and consulting on these types of offenses, this office has had numerous cases where the images alleged as child pornography were in fact not child pornography at all. In a federal case handled by my office in the District of Hawaii in 2002, United States v. Thomas Schnepfer, for instance the government alleged images in the defendant's computer as child pornography that were in fact images of adult pornography actress Melissa Ashley. This mistaken allegation triggered the necessity of a federal court order and my office received a copy of the defendant's hard drive. My firm's examination revealed that the images in question were not child pornography but actually Ms. Ashley yet even when the government was provided this information the child pornography allegations were not dropped necessitating Ms. Ashley's presence in court to testify regarding her identity in the images and her age. The child pornography charges were subsequently dismissed by the court, not the government.
37. Similar scenarios have occurred on other occasions with this firm, particularly where the allegation of child pornography is used by the government to bolster other (non pornography) charges against the defendant. The allegation of child pornography possession is used to "paint" the defendant as a deviant child predator to increase the odds of conviction when in reality, the images being used to do so are either not pornographic in nature (using current legal standards as related in U.S. v Dost) or, as was the case with defendant Schnepfer in Hawaii District Court, are actually of persons of legal age. In either scenario, it is the mere **allegation** that the images are child pornography that triggers this restrictive access to discovery and, in the experience of this firm, it would be naive to believe that the government does not take advantage of that fact at the defendant's expense.

## Previous Orders

38. This firm has been asked to address these issues and perform independent examinations of hard drives containing child pornography in numerous cases throughout the United States. The list of criminal cases below represents a portion of child pornography prosecutions wherein this firm was tasked via court order with the independent examination of hard drives containing child pornography at our laboratory facility. These examinations were done in Global CompuSearch's lab, independent of any prosecutorial or law enforcement presence and were safely and properly handled in every case:

- AZ v Jason Donald Simpson CR2003-019335-001 DT
- AZ v Craig Charles Rose # 2 CR2002-012446
- CA v Christian Kacher YA 049747
- CA v David Westerfield SCD165805
- CA v John Scott McClintock SCD162444
- CA v Kendell T. Ontko M01910070-2
- CA v Kurtis Brinkerhoff VCR168128
- CA v Roman Montiel FC-196731
- CA v Kenneth Williams F12750
- CA v Robert Pflieger GJ21408
- CO v Peter K. Dunn 02 CR 5218
- CO v Michael Gretzy 03CR2459
- CT v George Russell CR01-74313
- IL v Timothy Noonan 04 cf 3381
- MA v Randolph Roberge 0167 CR 2089
- MA v Richard Landau 2002-286-001/005
- NE v Samuel Thompson CR03-163
- NJ v Peter DiGiovanni 05-0300047-S
- NJ v Sean Fitzgerald 01-1944
- NY v Alexander Bueno-Edwards 03-1106
- NY v Brian Manzulo 203-2002
- NY v Warren Seper 03-0869
- OR v Steven Eric Gelhardt 0003613CR
- OR v David Waterstreet CR0400506 / 05-MC-9101
- US v Anthony Donadio CR03-40007
- US v Dennis Peterson CR01-5294FDD
- US v Chance Rearden CR 01-825-SVW
- US v SSgt E. Goodin US Court Marshall
- US v Droeder US Court Marshall
- US v Handel US Court Marshall
- US v A1C Howard US Court Marshall
- US v TSgt Fields US Court Marshall
- US v Bryan A. Nash Cr. S-04-0076-WBS
- US v Robert MacKenzie 03 -711 (JEI)

- US v Billy Smith 4:04 CR 141 SNL
- US v Justin Barrett Hill CR 02-1289-AK
- US v A1C Charles R. Phillips US Court Marshall
- OR v Sung Koo Sim C-04-1709-CR
- US In Re: Sung Koo Kim C-04-1709-CR
- US v Anthony Alexander 04-20005-BC
- US v Paul Greiner CR03-151-BLG-RFC
- US v Floyd T. Latta US Court Marshall
- US v Humberto Castaneda Padilla CR-03-1045-MMM
- US v Miriam Lawal CR-03-66-DDP
- US v David Michael Hill CR 02-1187-DDP
- US v Fallon Woodland CR 01-2003 JF
- US v James Edward Lee CR-F-02-5301 OWW
- US v Jeffery Scott Kuzdzal CR 03-12 Erie
- US v Jeffrey Brian Zeigler CR-03-08-BU-RFC
- US v John Lester CR02-6002FDB
- US v John Olinger
- US v Kenneth Young 04-CR-351-WM
- US v Kenneth King CR02-0376L
- US v Loren Samuel Williamson CR 02-60017-AA
- US v Michael Aaron Wilson CR02-6065FDB
- US v Robert Tashbook CR 01-20160 JF
- US v SSgt David T. Puckett Order and Stipulation, 18 MAR 2003
- US v Thomas M. Schnepfer 02-00062 HG
- US v Thomas Salinas CR 01-1029-AHM
- US v Wilson-Rutan, Andrew G Order dated 29 APR 2003
- US v Tony Guerrieri Order of Stipulation CR-03-144-GF-SHE
- US v Jarod D.D. Smith US Court Marshall
- US v Ronald Mikos 02 CR 137-1
- US v Hoover
- US v Robert William Crosbie 06-00047-CG
- US v William Heiser CR-04-0270
- US v David Shumaker
- US v SrA Luis Osorio
- US v SSGT John Lazard
- US v SrA Luis Osorio
- US v Daniel Brown
- US v Camnetar
- US v A1C Howard
- US v Tsgt Fields
- US v Rangel
- US v Shane Robert Ferguson CR 05-1154-JSL
- US v Jason Bilgere CR02870ERW
- US v Shannon Duncan CRS-04-022-WBS

- US v James Cannel CR-05-2059-EFS
- US v Bernnie Russell 03CR3283-JAH
- US v Tyrone Alan Gano CR-06-19-DSF
- US v John Mantos 06CR1416
- US v Gregory Vanausdel CR-04-20215JW
- US v Sharyar A. Raheem
- US v Kenneth Paul Wilk 04-60216-CR-COHN/SNO
- US v Willard Wm McDonough
- US v Ronnie Gurganusje 9:04-CR-58
- WA v Harjana Kioe 03-1-00006-4
- WA v James P. Degroff 02-1-0960-7
- WA v Thomas Lee Witkoski 02-1-03514-2
- WA v William Mannikko 01-1-697-0

39. Please note that this list is a small representation of court orders allowing this firm's temporary custody of contraband media and is by no means all-inclusive. It also does not include the numerous non-child pornography criminal cases that this office handles, notably, several capital homicide cases and the prosecution of Senior Airman Al Halabi for what was originally a death penalty espionage allegation by the United States Air Force.

#### **The Forensics Process Pre Trial**

40. It has been this firm's repeated experience that in preparing for trial, the forensics examination process is dynamic on both sides. As issues are raised by both sides in the release of Rule 16 and Jenks material, the claims of either must be verified or refuted by the experts. This can only be done by the defense if the defense expert has the ability to have repeated "as needed" access to the forensics copy of the computer media. In the investigative process described above, it is obvious why it would not be reasonable for an examiner to have to return to the government proscribed location continually throughout the dynamic process of release of discovery.
41. A government "on-site" approach also fails to consider the reality that the Redmond Police Department and other government facilities are not "open" to the public and will only allow non-agency access roughly between 9:00AM and 5:00PM. When we have attempted to do "on site" examinations in the past, this invariably is an issue since we are not allowed to "come and go" from a government office. It is very rare for examiners from this office to be able to confine their examination of a given hard drive or pieces of media to specific hours between 9:00AM and 5:00PM, and it is not unusual for Global CompuSearch's examiners to be doing forensics examinations of computer media well into the night and sometimes early-morning hours, particularly in the days leading up to trial. It is also not terribly uncommon for the government to hold off providing discovery at all until just days before trial (particularly in military prosecutions) necessitating an around the clock or weekend analysis. The examiners of this firm have attempted to work with the government in the past under constraints requiring "on site" examinations and found them unworkable for both Global CompuSearch and the government.

42. In an affidavit authored by Kevin Peden of my office regarding a recent attempted on-site evaluation at the Immigration and Customs Enforcement office in San Diego (August 9, 2006) he offered the following description;

"Based on the fact that the approval came late in the work day on August 8th, I was unable to leave Spokane Washington until August 9<sup>th</sup>, 2006 in the 0600 hour. Once there I drove to Camp Pendleton to meet with Capt Slabbekorn regarding the specifics of my duties on this examination. Up until my arrival in San Diego, I was under the impression that I would be conducting the examination on Camp Pendleton. I was planning on working from 0700 hours to 2200 hours each day in an attempt to complete this hasty examination. I was later advised by the Special agent Barnes, I.C.E. that the examination would take place in San Diego at the ICE office. I was also advised that this examination would have to be supervised by a federal agent.

Based on this information, Capt Slabbekorn and I contacted SA Barnes, ICE. We were assured that the supervision was necessary but that it would not intrude on the attorney client privileges afforded to the defense in this case. Barnes stated that they would be in the room but would not be watching what I was doing in the exam. During this conversation, SA Barnes asked what I needed from them and what time I was planning on working on the exam. I explained that I would need to work till about 2200 hours each night and begin by 0700 hours each morning. SA Barnes stated that he would see what he could do and let me know. I then left Camp Pendleton and drove to the San Diego office of ICE. I arrived there at approximately 1600 hours.

Once inside, SA Barnes escorted me to a large conference room and provided space to work at a conference table. He also provided one drive to begin with. This drive had the case files of 2 of the computer drives collected in this case as well as one power strip. SA Barnes advised me that he was told that his supervisor stated that ICE would not provide supervision except for the hours of 0830 – 1700 hours. He did state that he could stay a "little longer" if needed but not to 2200 hours. He also stated that he had attempted to make arrangements to have the media moved to Camp Pendleton for the examination so that the hours for my examination could be extended. He stated that he had been informed by "the powers that be" at Camp Pendleton, that this would not be afforded to the defense and that all examination would be done in San Diego at the ICE office. This greatly reduced the time afforded to the examination process. While we were discussing the time issues, SA Barnes stated, "I don't know what you can get done in this time, I have never done an investigation that fast". He also stated during my investigation that he spends at least 30 hours on most examinations.

I began my examination but experienced the following issues during the exam.

- The hours which I was allowed to work on the drive was 1600 – 1900 hours on August 9 and 0830 – 1700 hours on August 10, 11, 2005. I was able to begin the exams each day roughly at 0845 to 0900 hours after parking and setup were completed. Due to the limitation in time, I took a total of two, two minute restroom breaks and no other breaks on any of the days of examination. On

August 9<sup>th</sup> I stayed to around 1900 hours as SA Barnes stated that he would stay until that time. On August 10, I was able to start my exam around 0900 hours due to heavy traffic on I-5 from Oceanside to San Diego and parking issues. On August 11<sup>th</sup>, I left even earlier but found heavy traffic. I was able to start my examination around 0845 hours. I left the office on August 10 and 11 around 1700 hours. A complete investigation would have taken a week to a week and a half.

- Through the process, multiple agents were entering the room, talking to each other and on the phone. At one point I had 5 agents in the room. They were attempting to set up a computer for training uses next week. While they were in the room, one agent was roaming around near my attorney/client process to the point that I had to lock my computer several times to prevent the contents of the screen from being viewed.
- Throughout the investigation, I needed to converse with Capt Slabbekorn and my other examiners within my office but could not do so due to the supervision of ICE. Based on confidentiality issues surrounding my computer being left unattended, I felt that I needed to remain in the office at all times my computer was running. I was not in a secured office which would have afforded protection against the government reviewing it had the opportunity presented itself.
- Throughout the investigation, I needed internet access on a non-forensic computer for research. Due to the limitation of the examination area, this was not possible.
- During my investigation, several agents entered the room while I was working. They had many conversations, had paperwork spread out across a different conference and had many phone conversations. This was very distracting and made the investigation more difficult.
- During my investigation, I had case agents making phone calls to book their travel plans. This lasted nearly an hour.
- On Friday, during my investigation, Major Gleason, the prosecutor in this case arrived to check in with me on the progress of the investigation. He asked if I was going to be able to complete the investigation. I told him that I was about 18 hours into a 60 hour investigation and that there was no way a complete exam was possible under the circumstances. He relayed to me that he "sure hoped the case would not have to be continued"
- There were several times during my exam, that the supervising SA told me that I should reconsider working for the defense and come to work with the federal government."

43. I can state from repeated experience in attempting to work with the government "on-site" that my examiner Kevin Peden's experience is very typical. We are not provided privacy, we are not given the time we need we are not allowed to put in the hours necessary on a government time table and we do not have access to the tools we routinely need in the course of daily forensics examinations. In fact, it has been stated by agents from the Spokane ICE office that they do intend to physically observe examinations performed at their office.
44. It has been the repeated experience of Global CompuSearch examiners that when equal access is denied to the defense team, the prosecution is quick to exploit this in the courtroom and it is often presented to the fact finder as a lack of knowledge or preparation, when in reality, the defense has simply not had the same access to the media as the prosecution team.
45. These two overriding reasons, (1) the need to do examinations on our controlled, sterile and prepared machines in our own controlled laboratory environment with access to the other investigative tools present within it and (2) the continuing need to assess the media at the attorney's request in the days leading up to trial, are the primary reasons we, as a firm, made the determination that if we could not do examinations in our laboratory, we should not do them at all because to do so was a disservice to our clients and the persons they represent.

#### **Privacy Issues**

46. Another reality of an "on site" examination is that Global CompuSearch runs an active business that, as of this writing, has dozens of open cases. Our examiners routinely take calls and discuss private matters not only with the attorney whose case they may be currently examining, but with clients from literally all over the world, throughout the day, which is impossible to do when accompanied by a government agent able to overhear everything that is said.
47. In the affidavit filed by examiner Peden in my office mentioned above, he makes the following description related to his privacy during the examination process in the ICE offices in San Diego;

"Throughout the process, multiple agents were entering the room, talking to each other and on the phone. At one point I had 5 agents in the room. They were attempting to set up a computer for training uses next week. While they were in the room, one agent was roaming around near my attorney/client process to the point that I had to lock my computer several times to prevent the contents of the screen from being viewed.

Throughout the investigation, I needed to converse with Capt Slabbekorn and my other examiners within my office but could not do so due to the supervision of ICE. Based on confidentiality issues surrounding my computer being left unattended, I felt that I needed to remain in the office at all times my computer was running."

#### **Forensic Hardware**



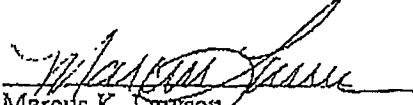
48. A government proposal for "on-site" examination also fails to take into account the eccentricities of working with electronic media. Our examiners have several times experienced damage to their forensic computers merely by transporting them on aircraft that rendered the machine unusable once the destination was reached. The reality is that desktop forensics machines must be checked as luggage when traveling on airliners which, in our experience invariably results in hardware problems at the destination and upon return.
49. This can be extremely frustrating as it is almost always our clients who have paid for our travel and that travel is virtually always limited to a minimum number of days. When the "on-site" examiner has to spend the first day of a two day exam (bearing in mind that when working in our laboratory we estimate 30 hours for the typical forensics exam) repairing a broken forensics machine, a competent examination becomes impossible.
50. Another reality also is that even "high tech" forensics computers sometimes refuse to work, go down and crash. When these problems occur, being separated from our Spokane office and additional forensics machines becomes a major problem.

### **Contraband Media Security**

51. As has repeatedly been explained in declarations, testimony and in person, this office never, under any circumstances, screen-captures or reproduces child pornography (or anything even closely resembling such) at any time or for any reason. The numerous court orders which have allowed us to possess mirror images of hard drives containing child pornography contraband have always specifically stated this, but even if they had not, this is the policy of Global CompuSearch.
52. Global CompuSearch is very familiar with the proper handling of computer evidence that has been deemed contraband. As stated above, I was previously employed with the government as a federal agent and has been entrusted with the storage and handling of child pornography evidence in child pornography/sex abuse cases on literally hundreds of occasions. I was, in fact, the assigned evidence custodian at my previous field office and the policies and procedures for evidence handling in this office have been created by me.
53. Global CompuSearch LLC specializes in the evaluation of computer evidence for litigation purposes. As such, all computer media is handled in a traditional law enforcement evidentiary manner. Global CompuSearch secures all such media in its digitally secure safes (which are located in a secured room within the office) between examinations with the appropriate court order attached. Evidence is removed from the safe only for evaluation and returned immediately upon any cessation of forensics work. As is this company's regular practice when receiving media in child pornography cases, Global CompuSearch request any drive(s) or other media to be marked by the technician making the forensics copy, the serial numbers are noted by Global CompuSearch and such drive(s) are wiped upon completion of the case, returned to law enforcement for wipe verification and a report of data destruction is provided to the attorney to file with the court.

54. As I have stated, I have been investigating child pornography crimes as either a federal agent or with my firm, Global CompuSearch, since 1989 and have seized, categorized and presented for prosecution thousands of images of child pornography going back to days even before computers to magazines and video tapes.
55. We request that evidentiary drives be shipped to our lab from the law enforcement entity making the copy (with an accompanying court order attached) via FedEx. As a firm, we have chosen FedEx for the shipping of media because of their superior package tracking system. From my prior government experience I know for a fact that government entities routinely use FedEx, UPS or DHL International for the purpose of delivering contraband media to and from other government offices. This procedure has been this firm's method of operation since our inception and this office has received and examined scores of computer hard drives containing child pornography contraband.
56. In many cases handled by Global CompuSearch, the government has previously conceded that contraband can be safely reviewed in our computer lab and a large number of court orders accompanying contraband media to our laboratory are the result of stipulations by the United States Attorneys Office and state prosecutors' offices throughout the country.
57. In those cases where release of media discovery was objected to by the government, and that media was subsequently received by this office via court order, there has *never* been an issue of loss or misuse of contraband. The orders as well provide for severe penalties should that be the case.
58. I also know from personal experience that it is not uncommon for prosecutors, including federal prosecutors to retain outside computer forensics expertise and release copies of contraband media to these experts. I am not privy to whether those releases included the government's obtaining a court order to do so.
59. I would submit that, in fact, many federal prosecutors and individuals in the Justice Department, as well as dozens of federal agents who have worked with this firm over the years are well aware that this firm is extraordinarily trust worthy with evidence.
60. Global CompuSearch prides itself, and in reality is based on, its honesty, its independence and its sensitivity to both the protection of children as well as the protection of the rights of accused persons. We inform counsel of all the facts we discover, both good and bad. This declaration is offered to the court with no other motive than to attempt to insure that both sides in these cases have equal access to the evidence in questions and arrive at the truth.
61. Again, the need to do examinations on our own forensics machines in the controlled laboratory environment of our offices including access to the other investigative tools present within it as well as the continuing need to assess the media at the attorney's request in the days leading up to trial, are the primary reasons we, as a firm, have previously made the determination that if we could not do examinations in our laboratory, we should not do them at all. We simply determined that to do examinations in any other way was a disservice to our clients and the persons they represent.

I swear under penalty of perjury that the foregoing is true.

  
Marcus K. Lawson  
President, Global CompuSearch

DATE: 11/10/07